RECEIVED
CENTRAL FAX CENTER
AUG 1 8 2004

FACSIMILE TRANSMISSION TO
THE UNITED STATES PATENT AND TRADEMARK OFFICE

OFFICIAL

DATE: 8/18/2004

RE: Serial No.: 09/517884

Docket No.: US00 8002

TO: Examiner: Zia, Mossadeq

Art Unit: 2134

Fax Number: (703) 872-9306

FROM: Michael J. Ure, Reg. No. 33,089

Telephone: (408) 474 - 9077

TRANSMISSION INCLUDES: 40 Pages (including cover sheet)

Brief for Appellant (in triplicate) - 39 pages

CERTIFICATE OF TRANSMISSION UNDER 37 CFR 1.8
I hereby certify that this correspondence is being facsimile transmitted to the Patent and Trademark Office at the number listed above
on 18-AUG 2004 by _____
Daniel L. Michalek

PHILIPS ELECTRONICS NORTH AMERICA CORPORATION
Intellectual Property & Standards
1109 McKay Drive M/S-41SJ
San Jose, California 95131
Fax Number: (408) 474-9082

PATENT
Attorney's Docket No. US00 8002

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

RECEIVED
CENTRAL FAX CENTER

AUG 1 8 2004

OFFICIAL

In re Patent Application of	
GEORGE FLEMING	Group Art Unit: 2134
Application No.: 09/517,884	Examiner: ZIA, MOSSADEQ
Filed: 03/03/2000	**Appeal No.**_____
For: IEEE 1394 LINK LAYER CHIP WITH "5C" AUTHENTICATION AND KEY EXCHANGE ACCELER- ATOR	

BRIEF FOR APPELLANT

BOX APPEAL BRIEF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This appeal is from the decision of the Primary Examiner dated 04/05/2004, finally rejecting claims 1-17, which are reproduced as an Appendix to this brief.

The Commissioner is authorized to charge the fee of $320, and any other fees that may be required by this paper, to Deposit Account No. 14-1270.

(1) Real Party in Interest

The real party in interest is the assignee, Koninklijke Philips Electronics, N.V.

(2) Related Appeals or Interferences

Applicant is not aware of any related appeals or interferences.

(3) Status of Claims

Claims 1-17 remain pending in the present application. All claims have been finally rejected and all claims are on appeal.

(4) Status of Amendments

All amendments have been entered. No amendment after final has been submitted.

(5) Summary of the Invention

The present invention may best be appreciated in relation to the field of consumer electronics. This field is very device-cost-sensitive. Furthermore, many such devices handle media content where the availability of media content may be a function of anti-piracy measures implemented to protect such media content. Finally, connectivity is an important attribute of such devices. Cryptographic functions important to media content protection such as key exchange, digital signature and digital signature verification are computation-intensive and require substantial processing power, power that is often unavailable to a consumer electronics device. To address this situation, according to one aspect of the present invention, such

functions are provided for in a link-layer access device, such as a 1394 ("Firewire") link-layer

access device (Figure 1, element 200; Figure 2), for example. A consumer electronics device

will often incorporate such a link-layer access device. In this manner, media content protection

may be achieved while maintaining low device cost, also while impacting device architecture

to a minimal degree.

(6) The References

The primary reference relied upon in rejecting the claims is Abraham, U.S. Patent

5,148,481. The system of Abraham is characteristic of the prior art described in the present

specification. Note that key exchange, digital signature and authentication are performed in

software (not in hardware as the term *device* connotes) on a PC. In particular, these functions

are performed by the security server program 117 of Abraham (col. 7, lines 30-40; Fig. 5). The

results of these functions are communicated to the cryptographic module 31 of the crypto-

graphic adapter hardware 29, e.g., in order for it to perform channel encryption/decryption.

A secondary reference, Sutikno, is combined with Abraham in rejecting various

ones of the dependent claims. Sutikno describes an arithmetic coprocessor for performing

elliptic curve cryptography. The coprocessor implements instructions (multiply, field inver-

sion, addition, input, output, rotate, copy, set) summarized in the second column of page 649 of

Sutikno.

(7) The Rejection

In the Final Rejection of October 23, 2002, claims 1-3, 5, 7 and 12 were rejected as

being anticipated by Abraham. Claims 4, 6, 8, 11, 15 and 17 were rejected as being unpatent-

able over Abraham in view of Sutikno. From paragraph 17 of the Final Office Action, is would

appear that the remaining claims (claims 9, 10, 13, 14 and 16) were also rejected as being

unpatentable over Abraham in view of Sutikno.

(8) Issue

The issues presented are: 1. Whether claims 1-3,5, 7 and 12 are anticipated by

Abraham; and 2. Whether the remaining claims would have been obvious in view of Abraham.

(9) Argument

The security server program 117 of Abraham cannot be equated to the link-layer access
device of claim 1.

Nor can the cryptographic adapter 29 of Abraham be equated to the link-layer access
device of claim 1. Although the cryptographic adapter does perform encryption/decryption, it
does not "provide, in response to one or more *commands* from the node controller, one or more
cryptographic items based on one or more *parameters* from the node controller."

Applicant notes that in the rejection of claim 1, the link-layer access device is identified
first as element 61 of Abraham (RS232 interface) and later as element 25 of Abraham
(workstation). Element 61 cannot be read as the link-layer access device of claim 1 because it
does not perform the recited functions of the link-layer access device of claim 1. Element 25
cannot be read as the link-layer access device of claim 1 because, if it does perform the recited

functions, performs them in software in like manner as the prior art, and not using a link-layer access *device* as claimed in claim 1.

Hence claims 1 and its dependent claims are believed to patentably distinguish over the cited references.

Claim 12 recites the corresponding method as claim 1 and, with its dependent claims, is believed to be patentable for similar reasons.

Claim 7, claiming a link-layer access *device,* and its dependent claims are believed to be patentable for similar reasons as claims 1 and 12. It is unreasonable to take the position that, because the *PC system* of Abraham may *contain* a link-layer access device, that the PC system *is* a link-layer access device. It is likewise unreasonable to take the position that any element within the *PC system* that performs a similar function as a function recited in the claim therefore satisfies that element.

Dependent claims 2-6, 8-11 and 13-17 are also believed to add novel and patentable subject matter to their respective dependent claims.

Claims 2, 3, 9, 10, 13 and 14 relate to particular cryptographic items provided by the link-access device in response to commands from the node controller. Neither Abraham nor Sutikno makes particular mention of these cryptographic items.

Claims 6, 11 and 17 relate to a particular set of commands issued by the node controller, including commands not made particular mention of in either Abraham or Sutikno.

Claim 4, 8 and 15 relate to deriving a second point on a elliptic curve from a first point on the elliptic curve and are applicable, for example, to Diffie-Hellman key exchange as described on page 6 of the specification. Such key exchange *per se* is well-known. However,

the combination of such features within the context of the independent claims is not believed to be taught or suggested by the cited references.

Claims 5 and 16 explicitly address key exchange. Once again, the combination of such features within the context of the independent claims is not believed to be taught or suggested by the cited references.
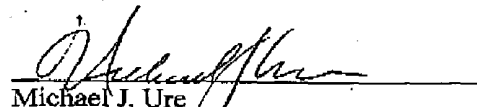
PATENT
Attorney's Docket No. US00 8002
Page 7

(10) CONCLUSION

For the foregoing reasons, claims 1-17 are believed to patentably define over the cited references.

Applicant respectfully submits therefore that the Final Rejection should be REVERSED.

Respectfully submitted,

Michael J. Ure
Attorney for Applicant
Registration No. 33,089

Date: August 18, 2004

APPENDIX OF CLAIMS

1. A processing system comprising:

an application device that is configured to communicate information with a physical-layer access device via a link-layer access device,

a node controller that is configured to control the link-layer access device,

the link-layer access device, operably coupled to the application device, the node controller, and the physical-layer access device, that is configured to facilitate an exchange of the information from and to the application device with data that is communicated to and from the physical-layer access device;

wherein,

the link-layer access device is further configured to provide, in response to one or more commands from the node controller, one or more cryptographic items based on one or more parameters from the node controller.

2. The processing system of claim 1, wherein

the one or more cryptographic items include at least one of:

a digital signature,

a verification of a digital signature, and

a cryptographic key item.

3. The processing system of claim 1, wherein

the one or more cryptographic items include:

a digital signature,

a verification of a digital signature, and

a cryptographic key item.

4. The processing system of claim 1, wherein

the link-layer access device includes a multiplication device that is configured to derive a second point on an elliptic curve from a first point on the elliptic curve, based on the one or more of the parameters from the node controller.

5. The processing system of claim 1, wherein

the node controller is configured to effect an exchange of a cryptographic key with another processing system, and

the one or more cryptographic items from the link-layer access device includes the cryptographic key.

6. The processing system of claim 1, wherein

the commands from the node controller include: a basepoint multiply command, a point multiply command, an EC-DSA verify command, and an EC-DSA sign command.

7. A link-layer access device comprising:

an application-layer interface device that is configured to communicate information with an application-layer device,

a physical-layer interface device that is configured to communicate data with a physical-layer device,

a buffer device, operably coupled to the application-layer interface device and the physical-layer interface device, that is configured to facilitate an exchange of the information of the application-layer device and the data of the physical-layer device,

a controller interface device, operably coupled to the application-layer interface device and the physical-layer interface device, that is configured to facilitate control of the exchange of information and data, and

an accelerator, operably coupled to a controller via the controller interface device, that is configured to compute one or more cryptographic items, in response to one or more cryptographic commands from the controller, and to thereafter communicate the one or more cryptographic items to the controller.

8. The link-layer access device of claim 7, wherein

the accelerator includes a multiplication device that is configured to derive a second point on an elliptic curve from a first point on the elliptic curve, based on one or more of parameters provided by the controller.

9. The link-layer access device of claim 7, wherein

the one or more cryptographic items includes at least one of:

a signature of a message,

a verification of a digital signature,

a hash of one or more parameters,

a random number,

an exponentiation of one or more parameters, and

an elliptic curve multiplication of one or more parameters,

the one or more parameters being provided by the controller.

10. The link-layer access device of claim 7, wherein

    the one or more cryptographic items include:

        a signature of a message,

        a verification of a digital signature, and

        an elliptic curve multiplication of one or more parameters,

    the one or more parameters being provided by the controller.

11. The link-layer access device of claim 7, wherein

    the one or more cryptographic commands include: a basepoint multiply command, a point multiply command, an EC-DSA Verify command, and an EC-DSA sign command.

12. A method for communications comprising:

communicating information from and to an application device to and from a physical-layer access device via a link-layer access device,

controlling the link-layer access device, in dependence upon commands from a node controller,

effecting an exchange of the information from and to the application device with data that is communicated to and from the physical-layer access device, and

determining one or more cryptographic items via computations within the link-layer access device, based on one or more parameters that are provided to the link-layer access device by the node controller.

13. The method of claim 12, wherein

the one or more cryptographic items include at least one of: .

a digital signature,

a verification of a digital signature, and

a cryptographic key item.

14. The method of claim 12, wherein

the one or more cryptographic items include:

a digital signature,

a verification of a digital signature, and

a cryptographic key item.

15. The method of claim 12, wherein

determining the one or more cryptographic items includes

deriving a second point on an elliptic curve from a first point on the elliptic curve, based on the one or more of the parameters from the node controller.

16. The method of claim 12, further including

effecting an exchange of a cryptographic key with an other processing system, wherein

the one or more cryptographic items from the link-layer access device includes the cryptographic key.

17. The method of claim 12, wherein

the commands from the node controller include: a basepoint multiply command, a point multiply command, an EC-DSA verify command, and an EC-DSA sign command.

<div align="right">
PATENT
Attorney's Docket No. US00 8002
</div>

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

RECEIVED
CENTRAL FAX CENTER

AUG 1 8 2004

OFFICIAL

In re Patent Application of	
GEORGE FLEMING	Group Art Unit: 2134
Application No.: 09/517,884	Examiner: ZIA, MOSSADEQ
Filed: 03/03/2000	Appeal No._____
For: IEEE 1394 LINK LAYER CHIP WITH "5C" AUTHENTICATION AND KEY EXCHANGE ACCELERATOR	

BRIEF FOR APPELLANT

BOX APPEAL BRIEF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This appeal is from the decision of the Primary Examiner dated 04/05/2004, finally rejecting claims 1-17, which are reproduced as an Appendix to this brief.

The Commissioner is authorized to charge the fee of $320, and any other fees that may be required by this paper, to Deposit Account No. 14-1270.

(1) Real Party in Interest

The real party in interest is the assignee, Koninklijke Philips Electronics, N.V.

(2) Related Appeals or Interferences

Applicant is not aware of any related appeals or interferences.

(3) Status of Claims

Claims 1-17 remain pending in the present application. All claims have been finally rejected and all claims are on appeal.

(4) Status of Amendments

All amendments have been entered. No amendment after final has been submitted.

(5) Summary of the Invention

The present invention may best be appreciated in relation to the field of consumer electronics. This field is very device-cost-sensitive. Furthermore, many such devices handle media content where the availability of media content may be a function of anti-piracy measures implemented to protect such media content. Finally, connectivity is an important attribute of such devices. Cryptographic functions important to media content protection such as key exchange, digital signature and digital signature verification are computation-intensive and require substantial processing power, power that is often unavailable to a consumer electronics device. To address this situation, according to one aspect of the present invention, such

functions are provided for in a link-layer access device, such as a 1394 ("Firewire") link-layer access device (Figure 1, element 200; Figure 2), for example. A consumer electronics device will often incorporate such a link-layer access device. In this manner, media content protection may be achieved while maintaining low device cost, also while impacting device architecture to a minimal degree.

(6) The References

The primary reference relied upon in rejecting the claims is Abraham, U.S. Patent 5,148,481. The system of Abraham is characteristic of the prior art described in the present specification. Note that key exchange, digital signature and authentication are performed in *software* (not in hardware as the term *device* connotes) on a PC. In particular, these functions are performed by the security server program 117 of Abraham (col. 7, lines 30-40; Fig. 5). The results of these functions are communicated to the cryptographic module 31 of the crypto-graphic adapter hardware 29, e.g., in order for it to perform channel encryption/decryption.

A secondary reference, Sutikno, is combined with Abraham in rejecting various ones of the dependent claims. Sutikno describes an arithmetic coprocessor for performing elliptic curve cryptography. The coprocessor implements instructions (multiply, field inversion, addition, input, output, rotate, copy, set) summarized in the second column of page 649 of Sutikno.

(7) The Rejection

In the Final Rejection of October 23, 2002, claims 1-3, 5, 7 and 12 were rejected as

being anticipated by Abraham. Claims 4, 6, 8, 11, 15 and 17 were rejected as being unpatentable over Abraham in view of Sutikno. From paragraph 17 of the Final Office Action, is would appear that the remaining claims (claims 9, 10, 13, 14 and 16) were also rejected as being unpatentable over Abraham in view of Sutikno.

(8) Issue

The issues presented are: 1. Whether claims 1-3,5, 7 and 12 are anticipated by Abraham; and 2. Whether the remaining claims would have been obvious in view of Abraham.

(9) Argument

The security server program 117 of Abraham cannot be equated to the link-layer access device of claim 1.

Nor can the cryptographic adapter 29 of Abraham be equated to the link-layer access device of claim 1. Although the cryptographic adapter does perform encryption/decryption, it does not "provide, in response to one or more *commands* from the node controller, one or more *cryptographic items* based on one or more *parameters* from the node controller."

Applicant notes that in the rejection of claim 1, the link-layer access device is identified first as element 61 of Abraham (RS232 interface) and later as element 25 of Abraham (workstation). Element 61 cannot be read as the link-layer access device of claim 1 because it does not perform the recited functions of the link-layer access device of claim 1. Element 25 cannot be read as the link-layer access device of claim 1 because, if it does perform the recited

functions, performs them in software in like manner as the prior art, and not using a link-layer access *device* as claimed in claim 1.

Hence claims 1 and its dependent claims are believed to patentably distinguish over the cited references.

Claim 12 recites the corresponding method as claim 1 and, with its dependent claims, is believed to be patentable for similar reasons.

Claim 7, claiming a link-layer access *device*, and its dependent claims are believed to be patentable for similar reasons as claims 1 and 12. It is unreasonable to take the position that, because the *PC system* of Abraham may *contain* a link-layer access device, that the PC system *is* a link-layer access device. It is likewise unreasonable to take the position that any element within the *PC system* that performs a similar function as a function recited in the claim therefore satisfies that element.

Dependent claims 2-6, 8-11 and 13-17 are also believed to add novel and patentable subject matter to their respective dependent claims.

Claims 2, 3, 9, 10, 13 and 14 relate to particular cryptographic items provided by the link-access device in response to commands from the node controller. Neither Abraham nor Sutikno makes particular mention of these cryptographic items.

Claims 6, 11 and 17 relate to a particular set of commands issued by the node controller, including commands not made particular mention of in either Abraham or Sutikno.

Claim 4, 8 and 15 relate to deriving a second point on a elliptic curve from a first point on the elliptic curve and are applicable, for example, to Diffie-Hellman key exchange as described on page 6 of the specification. Such key exchange *per se* is well-known. However,

the combination of such features within the context of the independent claims is not believed to be taught or suggested by the cited references.

Claims 5 and 16 explicitly address key exchange. Once again, the combination of such features within the context of the independent claims is not believed to be taught or suggested by the cited references.
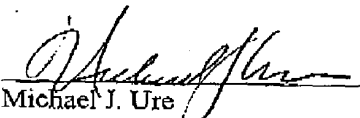
PATENT
Attorney's Docket No. US00 8002
Page 7

(10) CONCLUSION

For the foregoing reasons, claims 1-17 are believed to patentably define over the cited references.

Applicant respectfully submits therefore that the Final Rejection should be REVERSED.

Respectfully submitted,

Michael J. Ure
Attorney for Applicant
Registration No. 33,089

Date: August 18, 2004

APPENDIX OF CLAIMS

1. A processing system comprising:

an application device that is configured to communicate information with a physical-layer access device via a link-layer access device,

a node controller that is configured to control the link-layer access device,

the link-layer access device, operably coupled to the application device, the node controller, and the physical-layer access device, that is configured to facilitate an exchange of the information from and to the application device with data that is communicated to and from the physical-layer access device;

wherein,

the link-layer access device is further configured to provide, in response to one or more commands from the node controller, one or more cryptographic items based on one or more parameters from the node controller.

2. The processing system of claim 1, wherein

the one or more cryptographic items include at least one of:

a digital signature,

a verification of a digital signature, and

a cryptographic key item.

3. The processing system of claim 1, wherein

the one or more cryptographic items include:

a digital signature,

a verification of a digital signature, and

a cryptographic key item.

4. The processing system of claim 1, wherein

the link-layer access device includes a multiplication device that is configured to derive a second point on an elliptic curve from a first point on the elliptic curve, based on the one or more of the parameters from the node controller.

5. The processing system of claim 1, wherein

the node controller is configured to effect an exchange of a cryptographic key with an other processing system, and

the one or more cryptographic items from the link-layer access device includes the cryptographic key.

6. The processing system of claim 1, wherein

the commands from the node controller include: a basepoint multiply command, a point multiply command, an EC-DSA verify command, and an EC-DSA sign command.

7. A link-layer access device comprising:

an application-layer interface device that is configured to communicate information with an application-layer device,

a physical-layer interface device that is configured to communicate data with a physical-layer device,

a buffer device, operably coupled to the application-layer interface device and the physical-layer interface device, that is configured to facilitate an exchange of the information of the application-layer device and the data of the physical-layer device,

a controller interface device, operably coupled to the application-layer interface device and the physical-layer interface device, that is configured to facilitate control of the exchange of information and data, and

an accelerator, operably coupled to a controller via the controller interface device, that is configured to compute one or more cryptographic items, in response to one or more cryptographic commands from the controller, and to thereafter communicate the one or more cryptographic items to the controller.

8. The link-layer access device of claim 7, wherein

the accelerator includes a multiplication device that is configured to derive a second point on an elliptic curve from a first point on the elliptic curve, based on one or more of parameters provided by the controller.

9. The link-layer access device of claim 7, wherein

the one or more cryptographic items includes at least one of:

a signature of a message,

a verification of a digital signature,

a hash of one or more parameters,

a random number,

an exponentiation of one or more parameters, and

an elliptic curve multiplication of one or more parameters,

the one or more parameters being provided by the controller.

10. The link-layer access device of claim 7, wherein

the one or more cryptographic items include:

a signature of a message,

a verification of a digital signature, and

an elliptic curve multiplication of one or more parameters,

the one or more parameters being provided by the controller.

11. The link-layer access device of claim 7, wherein

the one or more cryptographic commands include: a basepoint multiply command, a

point multiply command, an EC-DSA Verify command, and an EC-DSA sign command.

12. A method for communications comprising:

communicating information from and to an application device to and from a physical-layer access device via a link-layer access device,

controlling the link-layer access device, in dependence upon commands from a node controller,

effecting an exchange of the information from and to the application device with data that is communicated to and from the physical-layer access device, and

determining one or more cryptographic items via computations within the link-layer access device, based on one or more parameters that are provided to the link-layer access device by the node controller.

13. The method of claim 12, wherein

the one or more cryptographic items include at least one of:

a digital signature,

a verification of a digital signature, and

a cryptographic key item.

14. The method of claim 12, wherein

the one or more cryptographic items include:

a digital signature,

a verification of a digital signature, and

a cryptographic key item.

15. The method of claim 12, wherein

    determining the one or more cryptographic items includes

        deriving a second point on an elliptic curve from a first point on the elliptic curve, based on the one or more of the parameters from the node controller.

16. The method of claim 12, further including

    effecting an exchange of a cryptographic key with an other processing system, wherein

    the one or more cryptographic items from the link-layer access device includes the cryptographic key.

17. The method of claim 12, wherein

    the commands from the node controller include: a basepoint multiply command, a point multiply command, an EC-DSA verify command, and an EC-DSA sign command.

PATENT
Attorney's Docket No. US00 8002

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

RECEIVED
CENTRAL FAX CENTER

AUG 1 8 2004

OFFICIAL

In re Patent Application of	
GEORGE FLEMING	Group Art Unit: 2134
Application No.: 09/517,884	Examiner: ZIA, MOSSADEQ
Filed: 03/03/2000	Appeal No._____
For: IEEE 1394 LINK LAYER CHIP WITH "5C" AUTHENTICATION AND KEY EXCHANGE ACCELER-ATOR	

BRIEF FOR APPELLANT

BOX APPEAL BRIEF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This appeal is from the decision of the Primary Examiner dated 04/05/2004, finally rejecting claims 1-17, which are reproduced as an Appendix to this brief.

The Commissioner is authorized to charge the fee of $320, and any other fees that may be required by this paper, to Deposit Account No. 14-1270.

(1) Real Party in Interest

The real party in interest is the assignee, Koninklijke Philips Electronics, N.V.

(2) Related Appeals or Interferences

Applicant is not aware of any related appeals or interferences.

(3) Status of Claims

Claims 1-17 remain pending in the present application. All claims have been finally rejected and all claims are on appeal.

(4) Status of Amendments

All amendments have been entered. No amendment after final has been submitted.

(5) Summary of the Invention

The present invention may best be appreciated in relation to the field of consumer electronics. This field is very device-cost-sensitive. Furthermore, many such devices handle media content where the availability of media content may be a function of anti-piracy measures implemented to protect such media content. Finally, connectivity is an important attribute of such devices. Cryptographic functions important to media content protection such as key exchange, digital signature and digital signature verification are computation-intensive and require substantial processing power, power that is often unavailable to a consumer electronics device. To address this situation, according to one aspect of the present invention, such

functions are provided for in a link-layer access device, such as a 1394 ("Firewire") link-layer

access device (Figure 1, element 200; Figure 2), for example. A consumer electronics device

will often incorporate such a link-layer access device. In this manner, media content protection

may be achieved while maintaining low device cost, also while impacting device architecture

to a minimal degree.

(6) The References

The primary reference relied upon in rejecting the claims is Abraham, U.S. Patent

5,148,481. The system of Abraham is characteristic of the prior art described in the present

specification. Note that key exchange, digital signature and authentication are performed in

software (not in hardware as the term *device* connotes) on a PC. In particular, these functions

are performed by the security server program 117 of Abraham (col. 7, lines 30-40; Fig. 5). The

results of these functions are communicated to the cryptographic module 31 of the crypto-

graphic adapter hardware 29, e.g., in order for it to perform channel encryption/decryption.

A secondary reference, Sutikno, is combined with Abraham in rejecting various

ones of the dependent claims. Sutikno describes an arithmetic coprocessor for performing

elliptic curve cryptography. The coprocessor implements instructions (multiply, field inver-

sion, addition, input, output, rotate, copy, set) summarized in the second column of page 649 of

Sutikno.

(7) The Rejection

In the Final Rejection of October 23, 2002, claims 1-3, 5, 7 and 12 were rejected as

being anticipated by Abraham. Claims 4, 6, 8, 11, 15 and 17 were rejected as being unpatent-able over Abraham in view of Sutikno. From paragraph 17 of the Final Office Action, is would appear that the remaining claims (claims 9, 10, 13, 14 and 16) were also rejected as being unpatentable over Abraham in view of Sutikno.

(8) Issue

The issues presented are: 1. Whether claims 1-3,5, 7 and 12 are anticipated by Abraham; and 2. Whether the remaining claims would have been obvious in view of Abraham.

(9) Argument

The security server program 117 of Abraham cannot be equated to the link-layer access device of claim 1.

Nor can the cryptographic adapter 29 of Abraham be equated to the link-layer access device of claim 1. Although the cryptographic adapter does perform encryption/decryption, it does not "provide, in response to one or more *commands* from the node controller, one or more *cryptographic items* based on one or more *parameters* from the node controller."

Applicant notes that in the rejection of claim 1, the link-layer access device is identified first as element 61 of Abraham (RS232 interface) and later as element 25 of Abraham (workstation). Element 61 cannot be read as the link-layer access device of claim 1 because it does not perform the recited functions of the link-layer access device of claim 1. Element 25 cannot be read as the link-layer access device of claim 1 because, if it does perform the recited

functions, performs them in software in like manner as the prior art, and not using a link-layer access *device* as claimed in claim 1.

Hence claims 1 and its dependent claims are believed to patentably distinguish over the cited references.

Claim 12 recites the corresponding method as claim 1 and, with its dependent claims, is believed to be patentable for similar reasons.

Claim 7, claiming a link-layer access *device*, and its dependent claims are believed to be patentable for similar reasons as claims 1 and 12. It is unreasonable to take the position that, because the *PC system* of Abraham may *contain* a link-layer access device, that the PC system *is* a link-layer access device. It is likewise unreasonable to take the position that any element within the *PC system* that performs a similar function as a function recited in the claim therefore satisfies that element.

Dependent claims 2-6, 8-11 and 13-17 are also believed to add novel and patentable subject matter to their respective dependent claims.

Claims 2, 3, 9, 10, 13 and 14 relate to particular cryptographic items provided by the link-access device in response to commands from the node controller. Neither Abraham nor Sutikno makes particular mention of these cryptographic items.

Claims 6, 11 and 17 relate to a particular set of commands issued by the node controller, including commands not made particular mention of in either Abraham or Sutikno.

Claim 4, 8 and 15 relate to deriving a second point on a elliptic curve from a first point on the elliptic curve and are applicable, for example, to Diffie-Hellman key exchange as described on page 6 of the specification. Such key exchange *per se* is well-known. However,

the combination of such features within the context of the independent claims is not believed to be taught or suggested by the cited references.

Claims 5 and 16 explicitly address key exchange. Once again, the combination of such features within the context of the independent claims is not believed to be taught or suggested by the cited references.
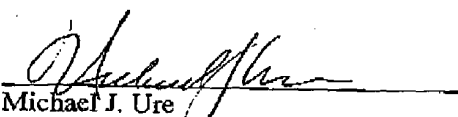
(10) CONCLUSION

For the foregoing reasons, claims 1-17 are believed to patentably define over the cited references.

Applicant respectfully submits therefore that the Final Rejection should be REVERSED.

Respectfully submitted,

Michael J. Ure
Attorney for Applicant
Registration No. 33,089

Date: August 18, 2004

APPENDIX OF CLAIMS

1. A processing system comprising:

an application device that is configured to communicate information with a physical-layer access device via a link-layer access device,

a node controller that is configured to control the link-layer access device,

the link-layer access device, operably coupled to the application device, the node controller, and the physical-layer access device, that is configured to facilitate an exchange of the information from and to the application device with data that is communicated to and from the physical-layer access device;

wherein,

the link-layer access device is further configured to provide, in response to one or more commands from the node controller, one or more cryptographic items based on one or more parameters from the node controller.

2. The processing system of claim 1, wherein

the one or more cryptographic items include at least one of:

a digital signature,

a verification of a digital signature, and

a cryptographic key item.

3. The processing system of claim 1, wherein

the one or more cryptographic items include:

a digital signature,

a verification of a digital signature, and

a cryptographic key item.

4. The processing system of claim 1, wherein

the link-layer access device includes a multiplication device that is configured to derive a second point on an elliptic curve from a first point on the elliptic curve, based on the one or more of the parameters from the node controller.

5. The processing system of claim 1, wherein

the node controller is configured to effect an exchange of a cryptographic key with an other processing system, and

the one or more cryptographic items from the link-layer access device includes the cryptographic key.

6. The processing system of claim 1, wherein

the commands from the node controller include: a basepoint multiply command, a point multiply command, an EC-DSA verify command, and an EC-DSA sign command.

7. A link-layer access device comprising:

an application-layer interface device that is configured to communicate information with an application-layer device,

a physical-layer interface device that is configured to communicate data with a physical-layer device,

a buffer device, operably coupled to the application-layer interface device and the physical-layer interface device, that is configured to facilitate an exchange of the information of the application-layer device and the data of the physical-layer device,

a controller interface device, operably coupled to the application-layer interface device and the physical-layer interface device, that is configured to facilitate control of the exchange of information and data, and

an accelerator, operably coupled to a controller via the controller interface device, that is configured to compute one or more cryptographic items, in response to one or more cryptographic commands from the controller, and to thereafter communicate the one or more cryptographic items to the controller.

8. The link-layer access device of claim 7, wherein

the accelerator includes a multiplication device that is configured to derive a second point on an elliptic curve from a first point on the elliptic curve, based on one or more of parameters provided by the controller.

9. The link-layer access device of claim 7, wherein

the one or more cryptographic items includes at least one of:

a signature of a message,

a verification of a digital signature,

a hash of one or more parameters,

a random number,

an exponentiation of one or more parameters, and

an elliptic curve multiplication of one or more parameters,

the one or more parameters being provided by the controller.

10. The link-layer access device of claim 7, wherein

    the one or more cryptographic items include:

        a signature of a message,

        a verification of a digital signature, and

        an elliptic curve multiplication of one or more parameters,

    the one or more parameters being provided by the controller.

11. The link-layer access device of claim 7, wherein

    the one or more cryptographic commands include: a basepoint multiply command, a point multiply command, an EC-DSA Verify command, and an EC-DSA sign command.

12. A method for communications comprising:

   communicating information from and to an application device to and from a physical-layer access device via a link-layer access device,

   controlling the link-layer access device, in dependence upon commands from a node controller,

   effecting an exchange of the information from and to the application device with data that is communicated to and from the physical-layer access device, and

   determining one or more cryptographic items via computations within the link-layer access device, based on one or more parameters that are provided to the link-layer access device by the node controller.

13. The method of claim 12, wherein

   the one or more cryptographic items include at least one of:

      a digital signature,

      a verification of a digital signature, and

      a cryptographic key item.

14. The method of claim 12, wherein

   the one or more cryptographic items include:

      a digital signature,

      a verification of a digital signature, and

      a cryptographic key item.

15. The method of claim 12, wherein

determining the one or more cryptographic items includes

deriving a second point on an elliptic curve from a first point on the elliptic curve, based on the one or more of the parameters from the node controller.

16. The method of claim 12, further including

effecting an exchange of a cryptographic key with an other processing system, wherein

the one or more cryptographic items from the link-layer access device includes the cryptographic key.

17. The method of claim 12, wherein

the commands from the node controller include: a basepoint multiply command, a point multiply command, an EC-DSA verify command, and an EC-DSA sign command.